Journal of Physical Security 3(1), 1-5 (2009)

Security Through Transparency:

An Open Source Approach to Physical Security

John P. Loughlin
Stanton Concepts
Lebanon, NJ
jpl@stantonconcepts.us

"Security through obscurity" has never been a sensible approach and now—with the Internet—is no longer achievable. A Google query on "lock picking" generates about 4,500,000 returns. There are about 10,000 videos on YouTube related to lock picking. Many bypass methods have gained wide attention including bumping and shimming as well as more sophisticated attacks on "high security" locks. Additionally, lock picking has become a popular sport. For example; www.locksport.com has 14 chapters in the US and Canada; Lockpicking 101 (www.lockpicking101.com) is a club with 60,000 members and its site has a forum to discuss and collaborate on picking and bypass techniques; The Open Organization Of Lock pickers (TOOOL) is based in The Netherlands and is the host and sponsor the annual Dutch Open lock picking competition. NDE (Non Destructive Entry) (www.ndemag.com) is an on line periodical that caters to the lock sport community. The lock sport community is composed predominantly of "white hats" that can play a vital role in the improvement of security hardware.

The general historic nature of the security hardware industry is to have their technology closed to the outside world. They are extremely averse to the hacking of their products and any revelation of vulnerabilities, real or perceived. The reasons for their position might include an obsolete mindset, a very large installed base of potentially vulnerable hardware, fear of tarnishing the brand name, and a diminished reputation for security products. In most cases, they can only delay, not prevent the inevitable; what is not revealed in the patents can be discovered by reverse engineering and will eventually be made public. The products that make the boldest claims tend to be the most inviting targets.

Even if a lock manufacturer discovered a vulnerability and chose to disclose the information; most deployed locks cannot be upgraded easily or in a cost-effective manner.

Stanton Concepts (SCI) has developed a new lock technology along with a new philosophic approach: the design information is open to the outside world.

Our lock cylinder employs well-known, time-tested, rotary mechanical lock mechanisms, while designing out many of the traditional vulnerability issues including bumping, picking, key control and key impressioning. There is no keyway to allow exploitation, observation, or manipulation of individual components. The key is designed with a novel means to manipulate the cylinder and provide management, control, and authorization features including audit trail (who, when, where etc.). The key is intended to change and improve as technology evolves. The resulting Robotic Key System (RKS) is a marriage of established mechanical elements with the new and ever changing state of electronic art.

To achieve these objectives, SCI decided that certain elements of the lock system should be Open Source. Open Sourcing has become increasingly common in software including IT security applications. Some of the more prominent Open Source software products include the Linux operating system, the Apache web server, and the Firefox web browser. The Open Source Software Initiative (OSI) is a non-profit organization that is actively involved in the Open Source community; their goal is to build and educate the community and meet with the public and private sectors to promote and discuss how Open Source Software technologies, licenses and development approaches can provide economic and strategic advantages.

OSI summarizes Open Source Software (OSS) on their website as:

"Open Source is a development method for software that harnesses the power of distributed peer review and transparency of process. The promise of open source is better quality, higher reliability, more flexibility, lower cost, and an end to predatory vendor lock-in."

OSI further defines Open Source Software as software that include these primary attributes; free distribution, inclusion of source code, no discrimination against persons or groups and no discrimination against fields of endeavor. Their definition also addresses licensing.

Open Source Hardware (OSH) is also becoming popular, including hardware for gaming, computer components, robotics, and telephony, but does not exist for security hardware. The term Open Source Hardware (OSH) primarily relates to hardware that is electronic in nature and implies the free release of the design information including schematics, bills of material, and PCB layout data. Open Source Software (OSS) is often used to drive the Open Source Hardware.

Predating both the Open Source software and hardware movements is an Open Source approach to cryptography which has been applied for years with great success. According to Bruce Schneier, (www.schneier.com), a leading expert in cryptography and computer security: "In the cryptography world, we consider Open Source necessary for good security; we have for decades. Public security is always more secure than proprietary security. It's true for cryptographic algorithms, security protocols, and security source code. For us, Open Source isn't just a business model; it's smart engineering practice."

The essential difference between software and hardware is that the hardware is a physical object that costs money to develop, prototype, manufacture and distribute. Software licenses rely on copyright law while hardware licenses rely on patent law.

The RKS has two primary elements; a mechanical lock cylinder and an electro-mechanical key. The key or Robotic Dialer includes electronic hardware and software. The cylinder is in the low-tech domain and the dialer is in the high tech domain.

The low-tech cylinder (figure 1) is a simple, stable, proven, and reliable lock mechanism that is highly resistant to manipulation. In addition, it has low cost and is environmentally robust. To quote Leonardo Da Vinci; "Simplicity is the ultimate sophistication". The cylinder can be a drop-in replacement for existing "high security" key cylinders; its form factor can be smaller or larger depending on the application.

Figure 1 - The low-tech RKS locking cylinder

The cylinder is a purely mechanical device that uses a combination type of lock mechanism. It has, however, a greater number of combinations ("keyspace") compared to conventional high security, manually operated combination locks. There is no keyway, and the lock cannot be finger-manipulated. The mechanical design yields several billion possible combinations. The assembly consists only of approximately 10 unique parts, with a total of about 30 parts overall, and is highly manufacturable. The RKS cylinder is currently commercially available in limited quantities.

A cylinder with 6 discs, each disc having 36 variations, theoretically yields 36^6 = 2,176,782,336 possible combinations. A 6-disc lock requires > 21 combined clockwise and counter-clockwise revolutions for alignment. The dialer in Figure 2 can dial a combination in about 3.5 seconds at an average RPM of 360. However, engineering may reduce the dialing to ~2 seconds. For example, if we reduce the number of combinations from $2.2X10^9$ to $1X10^9$, and assume 2 seconds per combination, it would take an adversary 6 years of brute-force sequential dialing to cycle through the entire keyspace. The mass and momentum of the lock mechanism also limits the speed of an attack.

The RKS Dialer used in conjunction with the cylinder is a portable electro-mechanical device that engages the cylinder. See figure 2. Once the Dialer user is authorized via a password or personal identification number (PIN), the dialer looks up the opening code in an onboard or remote database,

and then opens the lock by driving the cylinder's discs in the proper clockwise and counter-clockwise sequence.

Figure 2 - The RKS Dialer that unlocks the cylinder shown in figure 1.

Because the possible additional features and functions for the dialer are virtually limitless (GPS, biometrics, encryption, RFID, cellular and wireless etc.), the strategy is to provide a basic platform that includes an inexpensive and widely used PIC microcontroller (Microchip PIC16F917), motor controller, clock, EPROM, and a DC servomotor. The basic dialer can store a multitude of lock combinations. It uses PIN-based access control, has programmable time-out periods for specific locks and operators, and keeps a record of all activity. The dialer also has a USB interface to facilitate communication with a PC or Mac. This basic platform may be used for real world physical security applications, or as a development platform.

The Robotic Dialer is a natural for Open Source development. While the lock cylinders may be part of an installed base (perhaps located in uncontrolled environments), the dialer is portable and free to evolve independently and in real time. There is really no limit to the technology the Robotic Dialer could employ. The motor and dialing components could also be a subassembly designed to mate with an iPhone or other hand held computing device. Some or all of the management and control software could reside on the hand held device.

Currently, there are a number of advanced smart locks in the market place that involve a smart key that engages mechanically and electronically with a smart cylinder. These devices all use proprietary encryption schemes. Keeping the smart cylinders up-to-date with the latest software can be a challenge when the locks are deployed over a large area. Another concern is that once a crack or bypass is uncovered—either by reverse engineering, intellectual persistence, or application of new and sophisticated tools—the information can be distributed quickly, and every deployed lock will then be compromised.

Different users could develop Open Source hardware, software and encryption algorithms for the RKS dialer to meet their own specific needs and agendas. There could also be a collaborative effort among interested parties. Because the dialer is detached technologically from the cylinder, one party's dialer

would not have or (be able to) derive the opening information for another party's lock. The lock remains secure simply because of the extremely large number of possible permutations and the cylinder's intrinsic pick resistance. Also, unlike master key systems, disassembling one RKS lock cylinder reveals nothing about how the other RKS locks are combinated. As discussed above, determining the combination by sequential dialing is impractical because of the time required.

Of course there are pros and cons to Open Sourcing. The positive aspects include free software, transparent and available source code, community support, the fact that anyone can participate, security through many eyes, and the leveraging of a huge knowledge base. For security products, the only way to achieve a high degree of confidence is to have them examined by many experts. Another important positive aspect is that Open Sourcing gives companies that lack an Open Source approach an incentive to try harder to improve the security of their products.

Some of the negative aspects include licensing and IP issues, a complicated revenue model, lack of central control, issues associated with having many different versions of the same applications, documentation and support problems, and the fact that nefarious hackers have access as well as the end users.

There are several licensing models for both Open Source hardware and software products. In the case of the RKS, for example, Stanton Concepts could retain rights to the lock cylinder and mechanical interface. The lock cylinder would then be purchased or licensed, the dialer could also be purchased but the schematic, firmware, bill of material, and PCB data would be available under a Group Public License (GPL). The control software would also be Open Source, enabling users or organizations to develop and distribute software to suit their needs. Distinctions could also be made for commercial and non-commercial use.

In the view of Stanton concepts, the positive aspects of the Open Source approach far outweigh the negative. Open Sourcing allows interested parties to collaborate, continually improve, and expand the functionality and security of the lock system. The product is not constrained by one company's limited ability and/or closed architecture. The design would be more agile and vulnerabilities would be identified and hopefully addressed quickly and in a transparent manner.

Stanton Concepts agrees with Bruce Schneier in that not only is an Open Source approach a good business model, but it is also a smart engineering practice. The RKS is new and its future is uncertain, but we feel strongly that its unique design along with an Open Source approach bode well for its success.